PATENT APPLICATION
Docket No. 1384.2.3D

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :	John W.L. Ogilvie
Serial No.:	_____ (Division of 09/184,206)
Division Filed:	August 14, 2001
Title:	MESSAGE CONTENT PROTECTION AND CONDITIONAL DISCLOSURE
Parent Examiner:	Pierre Eddy Elisca (Art Unit 2161)

PRELIMINARY AMENDMENT

The Honorable Commissioner of
Patents & Trademarks
Washington, D.C. 20231

Commissioner:

Filed herewith is a divisional application based on commonly owned copending application serial no. 09/184,206 filed November 2, 1998, a true copy of which is filed concurrently. The inventor in this application is the same as in the '206 application.

Before calculating the fees in this divisional, please amend the application:

IN THE SPECIFICATION

In RELATED APPLICATIONS on page 1, please insert the following:

--This application is a division of United States Patent Application Serial No. 09/184,206 filed November 2, 1998. --

IN THE CLAIMS

Please cancel claims 1-18 and 54-62 without prejudice; those claims have been allowed in the parent application.

Claims 19-53 are presented here for examination.

Please amend independent claims 19 and 43 as shown below. This amendment is pursuant to an agreement reached during a telephone conference on August 14, 2001

between John Ogilvie and Examiner Pierre Eddy Elisca. The claims in the parent case were apparently allowed, among other reasons, because of the presence in independent claim 1 of a limitation directed to "hiding copies of sensitive information". During the telephone conference, it was agreed that adding corresponding express limitation language to claims 19 and 43 would be one way to make them allowable. Applicant still disagrees with the rejection of claims 19-53 in the parent application, but is willing to accept the claims below, and therefore respectfully requests that the claims presented here be allowed.

1-18. (deleted by this preliminary amendment)

19. (as originally filed in parent application, but showing changes made for this application) A computer system comprising a network, message storage means for storing in the network copies of a message, thereby hiding copies of sensitive information, and message disclosure means for disclosing the message if a predefined condition is detected.

19. (clean copy now presented in this divisional application) A computer system comprising a network, message storage means for storing in the network copies of a message, thereby hiding copies of sensitive information, and message disclosure means for disclosing the message if a predefined condition is detected.

20. The system of claim 19, wherein the message storage means comprises an encryption means for encrypting at least one message component.

21. The system of claim 19, wherein the message storage means comprises a digital signature means for digitally signing at least one message component.

22. The system of claim 19, wherein the message storage means comprises code to send a notice to a specified email address after the message has been stored.

23. The system of claim 19, wherein the message disclosure means comprises an email message generator for creating and mailing at least one email message containing a copy of at least a portion of the stored message.

24. The system of claim 19, wherein the message disclosure means comprises a web page generator for creating and posting at least a portion of a web page containing a copy of at least a portion of the stored message.

25. The system of claim 19, wherein the message disclosure means comprises code for detecting a deadman switch for triggering disclosure.

26. The system of claim 19, wherein the message disclosure means comprises code for detecting a reverse deadman switch for triggering disclosure.

27. The system of claim 19, wherein the network includes a local area network.

28. The system of claim 19, wherein the network includes a geographically dispersed network and at least two copies of the message are geographically dispersed in the network.

29. The system of claim 19, wherein the network includes nodes on different continents and at least two copies of the message are stored on different continents in the network.

30. The system of claim 19, further comprising a means for changing the location of message copies.

31. The system of claim 19, further comprising a means for placing message copies in at least one file disguise.

32. The system of claim 19, further comprising a message deletion means for deleting message copies.

33. The system of claim 32, wherein the message deletion means comprises a means for performing an emergency action in response to an apparent deletion request.

34. The system of claim 32, wherein the message deletion means comprises a cancellation means for deleting all stored message copies.

35. The system of claim 34, wherein the cancellation means requires authentication information which confirms that the source of the cancellation request is the same as the source of the message to be canceled.

36. The system of claim 19, further comprising a message update storage means for storing message updates.

37. The system of claim 36, wherein the message update storage means comprises code for creating decoy updates.

38. The system of claim 36, wherein the message update storage means comprises code for creating at least one secrecy renewal.

39. The system of claim 36, wherein the message update storage means comprises code for creating at least one address marker.

40. The system of claim 36, wherein the message update storage means comprises code for creating at least one searching update.

41. The system of claim 36, wherein the message update storage means comprises code for creating at least one update to a roving message.

42. The system of claim 36, wherein the message update storage means comprises code for creating at least one update to a poised message.

43. (as originally filed in parent application, but showing changes made for this application) A signal embodied in a network for controlled message disclosure, the signal comprising a sensitive information component which is hidden in the network and a disclosure condition component.

43. (clean copy now presented in this divisional application) A signal embodied in a network for controlled message disclosure, the signal comprising a sensitive information component which is hidden in the network and a disclosure condition component.

44. The signal of claim 43, wherein at least the sensitive information component is encrypted.

45. The signal of claim 43, wherein at least the sensitive information component is compressed.

46. The signal of claim 43, wherein at least the sensitive information component is digitally signed.

47. The signal of claim 43, further comprising a destination component.

48. The signal of claim 43, further comprising a disclosure format component.

49. The signal of claim 43, further comprising an identification component.

50. The signal of claim 43, further comprising a traveling program component.

51. The signal of claim 43, further comprising a deletion condition component.

52. The signal of claim 43, further comprising code for monitoring conditions to determine if disclosure or deletion is appropriate.

53. The signal of claim 52, wherein the code operates independently of any message update signals.

54-62. (deleted by this preliminary amendment)

Dated August 14, 2001.

Respectfully submitted,

\pm0prelim-3D

JOHN W.L. OGILVIE
Registration No. 37,987

COMPUTER LAW++
1211 East Yale Avenue
Salt Lake City, Utah 84105
(801) 582-2724 voice
(801) 583-1984 fax